Cybersicherheit: ENISA-Weißbuch: Können wir von industriellen Kontrollsystemen/SCADA-Zwischenfällen lernen?

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) veröffentlichte heute ein Weißbuch mit Empfehlungen zur Prävention und Bereitschaftsplanung für eine robuste und integrierte Reaktion auf Cyberangriffe und –attacken, die sich gegen industrielle Kontrollsysteme (ICS)/SCADA richten. Eine steigende Anzahl von sicherheitsrelevanten Vorfällen, welche auf industrielle Kontrollsysteme/SCADA abzielen, haben die Frage aufgeworfen, ob Organisationen die Möglichkeiten haben, auf diese Art von Angriffen zu reagieren, und ob generell ausreichend analytische Fähigkeiten vorhanden sind. Ein proaktives Lernumfeld mit Hilfe von Ex-Post-Analysen ist daher laut Agentur maßgeblich.

ICS wird generell für die Kontrolle von industriellen Prozessen wie Produktion, Fertigungsprozesse und Produktdistribution verwendet. Es wird jedoch leider häufig veraltete Standardsoftware eingesetzt. Bekannte ICS-Software beinhaltet u.a. sogenannte Control and Data Acquisition (SCADA), wobei SCADA die größte ICS-Untergruppe darstellt. Jüngste ICS/SCADA-Vorfälle unterstreichen den Stellenwert von Good Governance und Kontrolle von SCADA-Infrastrukturen. Besonders **die Fähigkeit auf sicherheitsrelevante Vorfälle zu reagieren, sowie die Kapazität die Folgen einer Attacke zu analysieren, um im Gegenzug von solchen Ereignisse zu lernen, sind besonders wichtig, betont die Agentur.**

Das Ziel einer Ex-Post-Analyse ist es, ein umfassendes Wissen über den Vorfall aufzubauen. Dieser Vorgang gibt Ihnen die Möglichkeit:

- sich auf konkrete Beweise zu stützen, um auf die sich ständig verändernde Art von inneren und äußeren Bedrohungen zu reagieren;
- sicherzustellen, dass ein ausreichender Lernprozess stattfindet um widerstandsfähige Systeme anzuwenden.

Wir haben vier Punkte für ein proaktives Lernumfeld identifiziert, welche im Gegenzug eine schnelle Reaktion auf Cyberbedrohungen und eine rasche Abwicklung der Ex-Post-Analysen gewährleistet:

- Vervollständigung der bereits existierenden Techniken von Ex-Post-Analysen und das Verständnis für die Überlappung zwischen virtuellen und nicht-virtuellen Critical Incident Response Teams;
- Vereinfachung der Integration von virtuellen und nicht-virtuellen Critical Incident Response Prozessen, sowie ein besseres Verständnis wo digitale Hinweise gefunden werden können und wie die passende Reaktion aussehen könnte;
- Systeme so zu designen und zu konfigurieren, dass diese eine digitale Beweissicherung ermöglichen; und
- Möglichkeiten die zwischenstaatliche und interorganisationalle Zusammenarbeit zu stärken.

Der Geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, kommentierte: „SCADA-Systeme sind oft Teil Sektoren, die zur wichtigen Infrastruktur eines Staates zählen, zum Beispiel bei der Stromversorgung und der Verkehrssteuerung, ein Umstand der diese Systeme besonders

attraktiv für Cyberattacken macht. Diese Attacken reichen von verärgerten Insidern zu Dissidentengruppen, bis hin zu fremden Staaten. Solche Systeme sollten so geführt werden, dass eine Sammlung und Analyse von digitalen Beweisen möglich ist, und somit Sicherheitsverletzungen besser identifizieren zu können."

Für den vollständigen Report und Tipps: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents
Für mehr Information: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
Für Interviews: Ulf Bergström, Pressesprecher, Telefon: ulf.bergstrom[at]enisa.europa.eu, Mobil: + 30 6948 460 143, oder Adrian Pauna, Experte, resilience[at]enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.
http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch
www.enisa.europa.eu